

# AUTHENTICATION METHOD FOR COUNTERFEIT PREVENTION, ITS EXECUTION SYSTEM, PROGRAM AND PROGRAM RECORDING MEDIUM

Publication number: JP2004342066

Publication date: 2004-12-02

Inventor: CHU CHIA-CHENG

Applicant: FAST ACCURATE DEVELOPMENTS LTD

Classification:

- international: B42D15/10; G06Q50/00; G07F7/08; B42D15/10;  
G06Q50/00; G07F7/08; (IPC1-7): B42D15/10;  
G06F17/60

- European: G06Q30/00C

Application number: JP20030298705 20030822

Priority number(s): TW20030113329 20030516

Also published as:

US 2004230528 (A1)

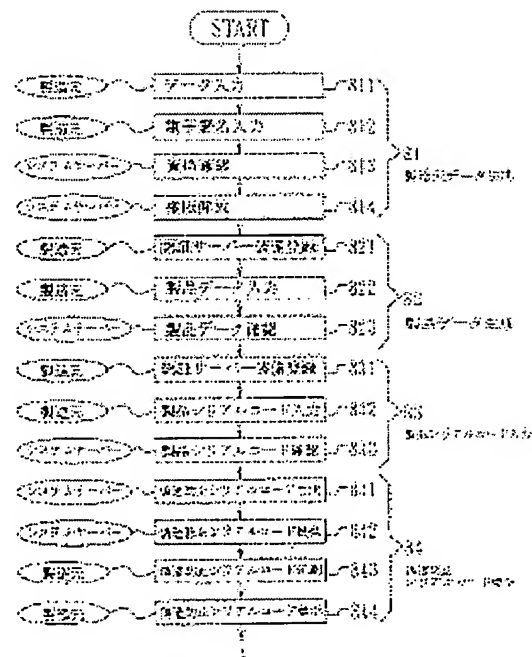
Report a data error here

## Abstract of JP2004342066

**PROBLEM TO BE SOLVED:** To provide an authentication method for counterfeit prevention reducing a risk of a consumer to buy a counterfeit.

**SOLUTION:** This authentication method for counterfeit prevention is provided with a product data input process (822) inputting product data by a manufacturer into authentication server equipment by product, an anti-counterfeit serial code generation process (841) generating a anti-counterfeit serial code corresponding to the product by the authentication server equipment, a serial code providing process (842) providing the anti-counterfeit serial code by the authentication server equipment to label the anti-counterfeit serial code on the product, a shipment/sale data input process inputting shipment/sale data of the product into the authentication server equipment, and a product authentication information providing process providing the product authentication information including at least shipment/sale data of the product corresponding to the anti-counterfeit serial code after receiving an authentication request by the anti-counterfeit serial code from the authentication server equipment.

COPYRIGHT: (C)2005,JPO&NCIPI



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-342066

(P2004-342066A)

(43) 公開日 平成16年12月2日(2004.12.2)

(51) Int. Cl.<sup>7</sup>G06F 17/60  
// B42D 15/10

F I

G06F 17/60 140  
G06F 17/60 154  
B42D 15/10 501P

テーマコード(参考)

2C005

審査請求 有 請求項の数 19 O L (全 11 頁)

(21) 出願番号 特願2003-298705 (P2003-298705)  
 (22) 出願日 平成15年8月22日(2003.8.22)  
 (31) 優先権主張番号 92113329  
 (32) 優先日 平成15年5月16日(2003.5.16)  
 (33) 優先権主張国 台湾(TW)

(特許庁注:以下のものは登録商標)

1. フロッピー

(71) 出願人 503304186  
 ▲鏡▼準開発有限公司  
 英国領バージン諸島 トルトーラ ロード  
 タウン オフショア インコーポレイシ  
 ョンズ センター ビーオー ボックス  
 957  
 (74) 代理人 100068755  
 弁理士 恩田 博宣  
 (74) 代理人 100105957  
 弁理士 恩田 誠  
 (72) 発明者 朱 家 正  
 台湾台北市基隆路1段111号9樓  
 Fターム(参考) 2C005 SA06 SA13

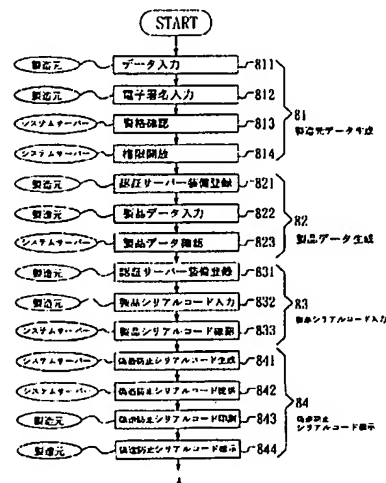
(54) 【発明の名称】 偽造品防止用認証方法、その実行システム、プログラム及びプログラム記録媒体

(57) 【要約】

【課題】 消費者が偽造品を買う危険性を低減させる偽造品防止用認証方法を提供する。

【解決手段】 偽造品防止用認証方法は、製造元による製品データを製品毎に認証サーバー装置に入力する製品データ入力工程(822)と、前記認証サーバー装置により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程(841)と、前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装置により、前記偽造防止シリアルコードを提供するシリアルコード提供工程(842)と、前記製品の出荷販売データを前記認証サーバー装置に入力する出荷販売データ入力工程と、前記認証サーバー装置により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程とを備える。

【選択図】 図3



## 【特許請求の範囲】

## 【請求項 1】

製造元による製品データを製品毎に認証サーバー装置に入力する製品データ入力工程と

前記認証サーバー装置により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、

前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装置により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、

前記製品の出荷販売データを前記認証サーバー装置に入力する出荷販売データ入力工程と、

前記認証サーバー装置により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程とを備えることを特徴とする偽造品防止用認証方法。

10

## 【請求項 2】

前記製品データ入力工程は、入力者の資格を確認するための認証を行うステップを第 1 のステップとして含むことを特徴とする請求項 1 に記載の偽造品防止用認証方法。

## 【請求項 3】

前記製品データ入力工程における製品データは、製造元、製品の名称、仕様、販売区域、製造日、推奨価格、製造地、使用期限、識別コード及び製造元の識別コードからなる群より選ばれた少なくとも一つを含んでいることを特徴とする請求項 1 に記載の偽造品防止用認証方法。

20

## 【請求項 4】

前記製品データ入力工程における製品データは、製品のシリアルコードを含んでおり、前記偽造防止シリアルコード生成工程における偽造防止シリアルコードは、前記製品のシリアルコードに応じて生成することを特徴とする請求項 1 に記載の偽造品防止用認証方法。

## 【請求項 5】

前記製品のシリアルコードは、製造元の識別コード、製品の識別コード、製造元から提供する偽造防止コードからなる群より選ばれた少なくとも一つを含んでいることを特徴とする請求項 4 に記載の偽造品防止用認証方法。

30

## 【請求項 6】

前記偽造防止シリアルコードは、前記製品のシリアルコードと同一であることを特徴とする請求項 4 に記載の偽造品防止用認証方法。

## 【請求項 7】

前記出荷販売データ入力工程の後のいずれかの段階に、前記認証サーバー装置によって前記出荷販売データの正否を確認する出荷販売データ確認工程を更に含むことを特徴とする請求項 1 に記載の偽造品防止用認証方法。

## 【請求項 8】

前記出荷販売データ確認工程は、確認者の資格を確認するための認証を行うステップを第 1 のステップとして含むことを特徴とする請求項 7 に記載の偽造品防止用認証方法。

40

## 【請求項 9】

前記出荷販売データ入力工程における出荷販売データは、販売先、販売先の識別コード、製品の出荷日からなる群より選ばれた少なくとも一つを含んでいることを特徴とする請求項 1 に記載の偽造品防止用認証方法。

## 【請求項 10】

前記製品認証情報は、前記製品データを更に含んでいることを特徴とする請求項 1 に記載の偽造品防止用認証方法。

## 【請求項 11】

前記製品認証情報は、製造元、製品の名称、仕様、製造日、使用期限、販売先からなる

50

群より選ばれた少なくとも一つを含んでいることを特徴とする請求項 10 に記載の偽造品防止用認証方法。

【請求項 12】

前記製品認証情報提供工程は、前記偽造防止シリアルコードによる認証請求の回数を累計するステップを含むことを特徴とする請求項 1 に記載の偽造品防止用認証方法。

【請求項 13】

前記製品認証情報提供工程が提供する製品認証情報は、前記偽造防止シリアルコードによる認証請求の回数を含んでいることを特徴とする請求項 12 に記載の偽造品防止用認証方法。

【請求項 14】

前記製品認証情報提供工程が提供する製品認証情報は、前記偽造防止シリアルコードによる前回の認証請求日時を含んでいることを特徴とする請求項 13 に記載の偽造品防止用認証方法。

【請求項 15】

前記製品認証情報提供工程は、前記偽造防止シリアルコードによる認証請求数が所定以上になると、異常警告を発するステップを含むことを特徴とする請求項 12 に記載の偽造品防止用認証方法。

【請求項 16】

製造元を前記製品データ入力工程及び前記販売データ入力工程における入力者とし、  
消費者を前記製品認証情報提供工程における認証請求者とし、  
販売先を前記出荷販売データ確認工程における確認者とすることを特徴とする請求項 1 ~ 15 のいずれかの一項に記載の偽造品防止用認証方法。

【請求項 17】

プログラムをロードした認証サーバー装置を備えている偽造品防止用認証システムであって、

前記認証サーバー装置は、前記プログラムに作動されて次の製造元による製品データを製品毎に認証サーバー装置に入力する製品データ入力工程と、

前記認証サーバー装置により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、

前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装置により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、

前記製品の出荷販売データを前記認証サーバー装置に入力する出荷販売データ入力工程と、

前記認証サーバー装置により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程を行うことを特徴とする偽造品防止用認証システム。

【請求項 18】

認証サーバー装置にロードされて前記請求項 1 ~ 15 のいずれかの一項に記載の偽造品防止用認証方法を前記認証サーバー装置に実行させるためのプログラム。

【請求項 19】

認証サーバー装置にロードされて前記請求項 1 ~ 15 のいずれかの一項に記載の偽造品防止用認証方法を前記認証サーバー装置に実行させるためのプログラムが記録されている記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、偽造品防止用認証方法、その偽造品防止用認証方法を実行するシステム、その偽造品防止用認証方法を実行するためのプログラム及びそのプログラムを記録する記録媒体に関する。

10

20

30

40

50

## 【背景技術】

## 【0002】

一般に、製造元から生産した製品は、認証された販売先や小売りを經由して消費者に販売される。前記販売先や小売りから渡された保証書により、消費者は、買い取った商品が偽造品ではなく、真正品であることを確保することができる。しかしながら、今では、電子交易及びネットワーク市場（サイバー市場）が普及すると共に、商品の偽造技術も日進月歩であると言えるので、消費者としては、前記販売先や小売りでなく他の販売通路から商品（中古品及び平行輸入商品を含む）を取得する時、偽造品を知らずに入手する危険性が非常に高い。また、消費者は、もともと商品の真偽を判断する能力があまりないのが通常であるので、販売先や小売りから保証書を手渡されても、商品の真否を疑う人が少なく

10

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0003】

上記に鑑みて、本発明は、消費者が偽造品を買い取る危険性を低減させ、それによって製造メーカや商社の商品販売システム及び名譽を確保することができる偽造品防止用認証方法及びその実行システム、プログラム、プログラム記録媒体を提供することを課題とする。

## 【課題を解決するための手段】

## 【0004】

前記課題を達成するために、まず、製造元による製品データを製品毎に認証サーバー装置に入力する製品データ入力工程と、前記認証サーバー装置により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装置により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、前記製品の出荷販売データを前記認証サーバー装置に入力する出荷販売データ入力工程と、前記認証サーバー装置により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程とを備えることを特徴とする偽造品防止用認証方法を提供する。

20

## 【0005】

それにより、消費者は、製品上の前記偽造防止シリアルコードに基づいて認証請求をし、そして、該製品に関わる認証情報を取った後、買おうとする商品または買い取ったところの商品が偽造品であるか否かを判断することができる。例えば、消費者が、A店に該商品を買ってから家に帰ると、インターネットで前記認証サーバー装置と繋ぎ、該商品に標示されている偽造防止シリアルコードを持って認証請求をし、もし該商品の出荷データにおいてA店への出荷が記載されていない場合、該商品は偽造品であると直ぐ判断できる。

30

## 【0006】

そして、また、偽造品防止用認証システムを提供する。該偽造品防止用認証システムは、プログラムをロードした認証サーバー装置を備えているものであって、前記認証サーバー装置は、前記プログラムに作動されて次の、製造元による製品データを製品毎に認証サーバー装置に入力する製品データ入力工程と、前記認証サーバー装置により、前記製品データと対応する偽造防止シリアルコードを生成する偽造防止シリアルコード生成工程と、前記製品上に前記偽造防止シリアルコードを標示するために、前記認証サーバー装置により、前記偽造防止シリアルコードを提供するシリアルコード提供工程と、前記製品の出荷販売データを前記認証サーバー装置に入力する出荷販売データ入力工程と、前記認証サーバー装置により、前記偽造防止シリアルコードによる認証請求を受けてから、前記偽造防止シリアルコードに対応する製品の少なくとも出荷販売データを含んでいる製品認証情報を提供する製品認証情報提供工程を行うことを特徴とする。

40

## 【0007】

さらに、認証サーバー装置にロードされて前記偽造品防止用認証方法を前記認証サーバ

50

一装置に実行させるためのプログラムを提供する。

さらに、認証サーバー装置にロードされて前記偽造品防止用認証方法を前記認証サーバー装置に実行させるためのプログラムが記録されている記録媒体を提供する。

【発明の効果】

【0008】

本発明の偽造品防止用認証方法、その実行システム、プログラム及びプログラム記録媒体によれば、消費者は、製品上の前記偽造防止シリアルコードにより認証請求を行って該製品の認証情報を取ることができるので、買おうとする商品または買ったばかりの商品が偽造品であるか否かを判別することができる。したがって、消費者が偽造品を買う危険性を大幅に低減し、製造元または販売商社の販売ルート及び会社の名誉を確保することができ

10

【発明を実施するための最良の形態】

【0009】

以下、本発明の好ましい実施形態を詳しく説明する。この実施形態の偽造品防止用システム100は、図1に示すように、主として認証サーバー装置1と、製造元で使用される製造元の端末装置2と、販売先で使用される販売先の端末装置3と、認証請求プロキシサーバー4と、消費者に使用される消費者の端末装置5とを備える。製造元及び販売先の端末装置2、3は、それぞれ情報ネットワーク61、62を介して認証サーバー装置1と接続されている。消費者の端末装置5は、情報ネットワーク63及び認証請求プロキシサーバー4を介して認証サーバー装置1と接続されている。それにより、製造元、販売先及び消費者の端末装置2、3、5からデータを認証サーバー装置1に伝送させることができる。

20

【0010】

本実施形態における認証サーバー装置1は、分散式フレームワーク構成を有する上、システムサーバー11と、メインデータベース12と、バックアップ用データベース13と、製造元のサーバー14と、販売先のサーバー15と、認証請求のサーバー16とを備える。

【0011】

システムサーバー11内には、認証サーバー装置1を管理するに必要な操作システム及び応用プログラムが設けられている。認証サーバー装置1のシステム管理人は、システムサーバー11により管理を行うことができる。本実施形態において、メインデータベース12及びバックアップ用データベース13として、ハードディスクが使用されている。また、それに限らず、メインデータベース12及びバックアップ用データベース13として、フロッピーディスクや磁性テープなどの磁気記録媒体、光ディスクなどの光学記録媒体、他の固定式または可動式テープ記録媒体が使用されてもよい。

30

【0012】

図2に示すように、メインデータベース12は、製造元のデータ121、製品データ122、製品シリアルコード123、偽造防止シリアルコード124、販売先のデータ125、出荷販売データ126、製品認証情報127、認証請求記録128を記憶している。製造元のデータ121、製品データ122、製品シリアルコード123、出荷販売データ126は、製造元の端末装置2からメインデータベース12に送信され、販売先のデータ125は、販売先の端末装置3からメインデータベース12に送信され、偽造防止シリアルコード124は、システムサーバー11からメインデータベース12に送信される。また、システムサーバー11から受信した偽造防止シリアルコード124は、製造元の端末装置2に送信される。

40

【0013】

そして、認証請求記録128は、認証請求プロキシサーバー4から前記メインデータベース12に送信される。該認証請求プロキシサーバー4から受信した認証請求記録128は、製造元及び販売先の端末装置2、3に提供される。製品認証情報127は、製品データ122、出荷販売データ126及び認証請求記録128から生成し、且つ認証請求プロ

50

キシサーバー 4 に提供される。バックアップ用データベース 13 は、システムサーバー 11 の制御によりメインデータベース 12 に記憶されたデータのバックアップを自動かつ定期的に行うように機能する。

【0014】

なお、図 1 に示すように、ネットワークの安全性のために、製造元のサーバー 14、販売先のサーバー 15 及び認証請求プロキシサーバー 4 と製造元の端末装置 2、販売先の端末装置 3 及び消費者の端末装置 5 との間に、外部防火壁 71 が設けられている。製造元のサーバー 14、販売先のサーバー 15 及び認証請求のサーバー 16 とシステムサーバー 11、メインデータベース 12 及びバックアップ用データベース 13 との間に、内部防火壁 72 が設けられている。

10

【0015】

外部防火壁 71 と内部防火壁 72 との間に、認証サーバー装置 1 を保護して製造元の端末装置 2 や販売先の端末装置 3、消費者の端末装置 5 からの悪意侵入や攻撃を避ける非武装地帯 (DMZ) 73 が形成されている。

【0016】

前記防火壁の設置は公知技術であり、且つ本発明の特徴と関係がないので、その詳しい説明を省略する。

製造元のサーバー 14、販売先のサーバー 15 及び認証請求のサーバー 16 は、それぞれ製造元の端末装置 2、販売先の端末装置 3 及び消費者の端末装置 5 と接続されている。また、製造元のサーバー 14、販売先のサーバー 15 及び認証請求のサーバー 16 は、メインデータベース 12 と接続されている。それにより、端末装置 2、3、5 からのデータ及び認証請求をサーバー 14、15、16 を介してメインデータベース 12 にアップロードしたり、メインデータベース 12 からサーバー 14、15、16 を介してデータを端末装置 2、3、5 にダウンロードしたりすることができる。

20

【0017】

本実施形態において、製造元の端末装置 2 及び販売先の端末装置 3 として、パーソナルコンピュータが使用され、情報ネットワーク 61、62 として、インターネットが使用されているが、それに限らず、情報ネットワーク 61、62 として、例えば、広域ネットワーク (WAN)、構内ネットワーク (LAN) が使用されてもよい。また、情報ネットワーク 61、62 は、非対称デジタル加入者線 (ADSL) モデム、ダイヤルアップ式モデム、広帯域ケーブルモデムによって、統合デジタルサービル通信網 (ISDN) 回線、T1 専用回線、他の有線や無線の接続回線で構築されることができる。

30

【0018】

図 1 に示すように、消費者の端末装置 5 として、例えば、パーソナルコンピュータ 51、携帯用情報端末 (PDA) 52、携帯電話 53、一般の電話 54、ファックスマシン 55 が挙げられる。端末装置 51～55 は、それぞれ有線のインターネット接続 631、無線のインターネット接続 632、例えば汎用パケット無線システム (GPRS) 及び符号分割多元接続 (CDMA) システムなどの携帯電話の接続ネットワーク 623、音声情報伝送用の公衆電話交換網 (PSTN) システム 624、テキスト情報伝送用の公衆電話交換網 (PSTN) システム 625 を介して認証請求プロキシサーバー 4 と接続されている。

40

【0019】

前記配置により、消費者 (認証請求者) は、任意の場所、任意の時間に各種の端末装置 51～55 を自由地使用し、端末装置 5 を経由して認証請求を行って製品の認証情報を取得することができる。例えば、パーソナルコンピュータ 51 または携帯用情報端末 (PDA) 52 により有線または例えばブルートゥースなどの無線の接続を介してオンライン認証請求を行い、携帯電話 53 により無線アプリケーション・プロトコル (WAP) またはショートメッセージを介して認証請求を行い、一般の電話 54 によりキーパッド制御の方式で自動コールアテンダントサービスを介して認証請求を行い、ファックスマシン 55 によりテキストの方式でファックス自動回答サービスを介して認証請求を行うことができ

50

る。

#### 【0020】

以下、図2～図4を参照しながら、図1のような偽造品防止用認証システムによる偽造品防止用認証方法を説明する。この偽造品防止用認証方法は、主として製造元のデータ121を生成する製造元データ生成工程81と、製品データ122を生成する製品データ生成工程82と、製品シリアルコード123を入力する製品シリアルコード入力工程83と、偽造防止シリアルコード124を標示する偽造防止シリアルコード標示工程84と、販売先のデータ125を生成する販売先データ生成工程85と、製品の出荷販売データ126を生成する出荷販売データ生成工程86と、製品認証請求を行う製品認証請求工程87とからなる。

10

#### 【0021】

製造元データ生成工程81は、四つのステップ811～814を有する。まず、製造元は、システム管理者と協力して認証サーバー装置1に登録して製造元のデータ121を入力する。製造元のデータ121は、メインデータベース12に記憶される。本実施形態において、製造元のデータ121は、製造元の識別コード（ID、例えばインボイスコード）、パスワード、電子署名、名称、基本資料（例えば電話番号、ファックス番号、eメールアドレス、住所アドレスなど）、権限、所在地を含んでいる。そして、製造元は、端末装置2の使用ユーザーインターフェイス（例えばインターネットブラウザ）により製造元のサーバー14を介してメインデータベース12に入って電子署名を入力する。システムサーバー11は、製造元の資格を確認する。確認完成后、製造元の権限が開放され、製造元が

20

#### 【0022】

製品データ生成工程82は、三つのステップ821～823を有する。まず、製造元は識別コード及びパスワードにより認証サーバー装置1に登録する。登録が成功した後、製品データ122を製品毎に認証サーバー装置1に入力する。製品データ122は、主として製品の特徴を描く。本実施形態において、製品データ122は、製造元、製品の名称、仕様（例えば寸法、重さ、外形、体積、色など）、販売区域、製造日、推奨価格、製造地、使用期限、識別コード及び製造元の識別コードを含んでいる。そして、システムサーバー11は、製品データ122の完成度を確認し、確認した後、メインデータベース12に記憶する。

30

#### 【0023】

製品シリアルコード入力工程83は、三つのステップ831～833を有する。まず、製造元は識別コード及びパスワードにより認証サーバー装置1に登録する。登録が成功した後、製品データ122と対応する製品シリアルコード123を製品毎にメインデータベース12に入力する。本実施形態において、製品シリアルコード123は、製造元の識別コード、製品の識別コード、販売先の識別コード、製造元から提供する偽造防止コード、システムサーバー11のプログラムから提供する認証コードを含んでいる。そして、システムサーバー11は、製品シリアルコード123の完成度を確認し、確認した後、メインデータベース12に記憶する。

40

#### 【0024】

偽造防止シリアルコード標示工程84は、四つのステップ841～843を有する。まず、システムサーバー11は、製品シリアルコード123に応じて偽造防止シリアルコード124を生成してメインデータベース12に記憶する。偽造防止シリアルコード124は、製品シリアルコード123と完全的または部分的に同じでも良く、製品シリアルコード123と特殊な関係を有する独特の符号、数字、文字及びそれらの組合せでも良い。図5は、偽造防止シリアルコード124の一例を示す説明図である。図5中の該偽造防止シリアルコード124におけるMS、W95、TW01、15200は、それぞれ製造元の識別コード、製品の識別コード、販売先の識別コード、偽造防止コードを示している。

#### 【0025】

そして、システムサーバー11は、前記偽造防止シリアルコード124を前記製造元の

50



端末装置 2 に送信する。前記製造元は、前記偽造防止シリアルコード 1 2 4 を印刷し、対応の製品に標示する。

【0026】

図 6 は、図 5 の偽造防止シリアルコード 1 2 4 を製品 1 0 1 に標示した時の斜視図である。図 6 に示すような例は、記図 5 の偽造防止シリアルコード 1 2 4 が空白のラベルに印刷されてから製品 1 0 1 上に貼り付けられる方式であるが、それに限らず、マシン読み出し可能のタイプに作ってもよい。

【0027】

そして、販売先のデータ生成工程 8 5 は、四つのステップ 8 5 1 ～ 8 5 4 を有する。まず、販売先は、システム管理者と協力して認証サーバー装置 1 に登録して販売先のデータ 1 2 5 を入力する。販売先のデータ 1 2 5 は、メインデータベース 1 2 に記憶される。本実施形態において、販売先のデータ 1 2 5 は、販売先の識別コード（ID、例えばインボイスコード）、パスワード、電子署名、名称、基本資料（例えば電話番号、ファックス番号、e メールアドレス、住所アドレスなど）、権限、所在地を含んでいる。そして、販売先は、端末装置 3 の使用者インターフェイス（例えばインターネットブラウザ）により販売先のサーバー 1 5 を介してメインデータベース 1 2 に入って電子署名を入力する。システムサーバー 1 1 は、販売先の資格を確認する。確認完成后、販売先の権限を開放し、販売先が認証サーバー装置 1 を操作することができる。

10

【0028】

出荷販売データ生成工程 8 6 は、七つのステップ 8 6 1 ～ 8 6 7 を有する。製造元は、製品を販売先に出荷した後、製品上の偽造防止シリアルコード 1 2 4 により認証サーバー装置 1 に登録して出荷販売データ 1 2 6 を認証サーバー装置 1 に入力してメインデータベース 1 2 に記憶する。

20

【0029】

本実施形態において、出荷販売データ 1 2 6 は、製品のシリアルコード、識別コード、製造元の識別コード以外に、販売先、販売先の識別コード、製品の出荷日、製造元の確認シリアルコード、販売先の確認シリアルコード、システムサーバー 1 1 のプログラムに識別される販売確認シリアルコードを含んでいる。そして、製品が入荷した後、販売先は、製品上の偽造防止シリアルコード 1 2 4 により製品毎に認証サーバー装置 1 に登録して対応の出荷販売データ 1 2 6 を取り、出荷販売データ 1 2 6 の正否を確認する。そして、販売先は、該製品を消費者に販売する。

30

【0030】

製品認証請求工程 8 7 は、六つのステップ 8 7 1 ～ 8 7 6 を有する。まず、消費者は、認証請求プロキシサーバー 4 に認証された端末装置 5 の使用者インターフェイス（例えばインターネットブラウザ）により製品上の偽造防止シリアルコード 1 2 4 を入力して認証請求を行う。そして、認証請求プロキシサーバー 4 はメインデータベース 1 2 から偽造防止シリアルコード 1 2 4 と対応する製品認証情報 1 2 7 を取得する。

【0031】

本実施形態において、製品認証情報 1 2 7 は、製造元、製品の名称、仕様、製造日、使用期限、販売先、偽造防止シリアルコード 1 2 4 による認証請求の累計回数、前記偽造防止シリアルコードによる前回の認証請求日時を含んでいる。

40

【0032】

そして、認証請求プロキシサーバー 4 は、製品認証情報 1 2 7 を消費者の端末装置 5 に提供する。消費者は、製品認証情報 1 2 7 に基づいて製品の真偽を判別することができる。例えば、同一の偽造防止シリアルコード 1 2 4 による認証請求の回数が異常である時、該製品が偽造される可能性があることが判る。

【0033】

そして、認証請求プロキシサーバー 4 は、認証請求記録 1 2 8 を自動的に更新すると共に製品認証情報 1 2 7 を更新する。本実施形態において、認証請求記録 1 2 8 は、製品シリアルコード 1 2 3、認証請求回数、認証請求日時、請求元（例えば IP アドレス）、異

50

常かどうか（偽造防止シリアルコードによる認証請求数が所定以上になる）、製品状況（例えば、製品の現在位置、使用期限）を含んでいる。

#### 【0034】

次に、認証請求プロキシサーバー4は、認証請求記録128を製造元の端末装置2及び販売先の端末装置3に定期的送信し、製造元及び販売先は、認証請求記録128に基づいて偽造の発生があるかどうかを判別することができる。また、偽造防止シリアルコード124による認証請求数が所定以上になると、ショートメッセージで製造元及び販売先に異常警告を発するように機能させることもできる。

#### 【産業上の利用可能性】

#### 【0035】

上記のように、本発明の偽造品防止用認証方法及びその実行システムによれば、消費者が商品の認証情報を容易に取得して商品の真偽を判別することができるので、偽造品を買う危険性を大幅に低減させることができる。また、製造元及び販売先は、前記認証請求記録に基づいて製品が偽造されるかどうかを判別することができるので、商品が偽造される恐れを低減させることができる。即ち、消費者と製造元と販売先との三者の権利を守ることができる。

#### 【0036】

そして、前記偽造品防止用認証方法及びその実行システムに基づき、本発明は、前記認証サーバー装置にロードされるプログラム及び前記プログラムが記録されている記録媒体を提供することができる。即ち、本発明の偽造品防止用認証システムは、一般のコンピュータ及び今に普及しているインターネットと配合し、低いコストで実行されることができる。

#### 【0037】

以上説明した実施の形態は、あくまでも本発明の技術的内容を明らかにする意図のものにおいてなされたものであり、本発明はそうした具体例に限定して狭義に解釈されるものではなく、本発明の精神とクレームに述べられた範囲で、いろいろと変更して実施できる。

#### 【図面の簡単な説明】

#### 【0038】

【図1】本発明の一実施形態にかかる偽造品防止用システムの概略的な構成図。

【図2】メインデータベースと他の装置との関係のブロック図。

【図3】本発明の偽造品防止用認証方法の好ましい実施形態のフローチャート。

【図4】同じく偽造品防止用認証方法の好ましい実施形態のフローチャート。

【図5】偽造防止シリアルコードの一例の説明図。

【図6】図5の偽造防止シリアルコードを製品上に標示した時の斜視図。

#### 【符号の説明】

#### 【0039】

100	偽造品防止用システム
101	製品
1	認証サーバー装置
11	システムサーバー
12	メインデータベース
121	製造元のデータ
122	製品データ
123	製品シリアルコード
124	偽造防止シリアルコード
125	販売先のデータ
126	出荷販売データ
127	製品認証情報
128	認証請求記録

10

20

30

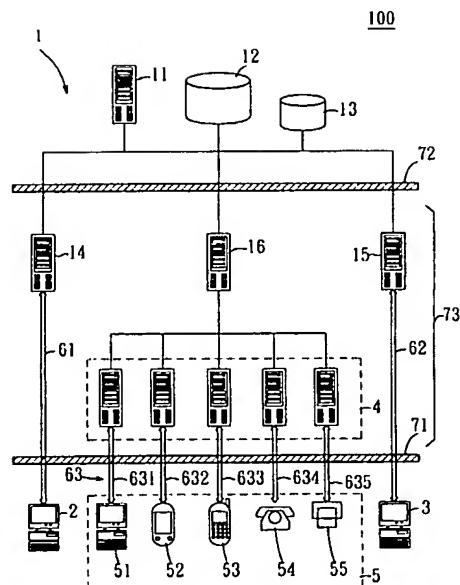
40

50

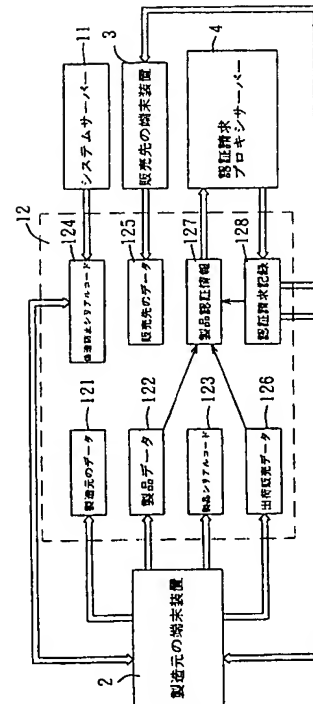
- 1 3      バックアップ用データベース
- 1 4      製造元のサーバー
- 1 5      販売先のサーバー
- 1 6      認証請求のサーバー
- 2      製造元の端末装置
- 3      販売先の端末装置
- 4      認証請求プロキシサーバー
- 5, 5 1 ~ 5 5      消費者の端末装置
- 6 1 ~ 6 3      情報ネットワーク
- 6 3 1 ~ 6 3 5      情報ネットワーク
- 7 1      外部防火壁
- 7 2      内部防火壁
- 7 3      非武装帯域

10

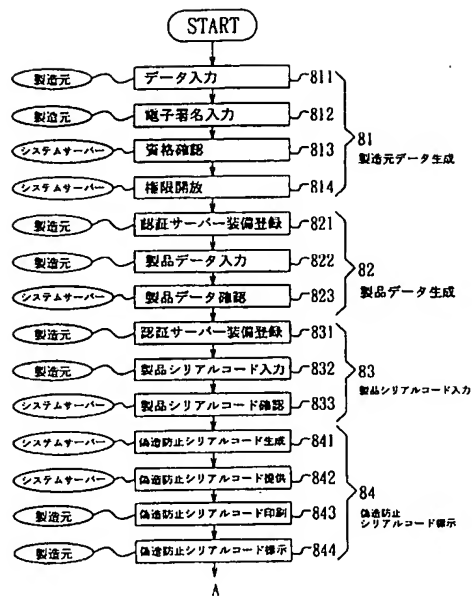
【図 1】



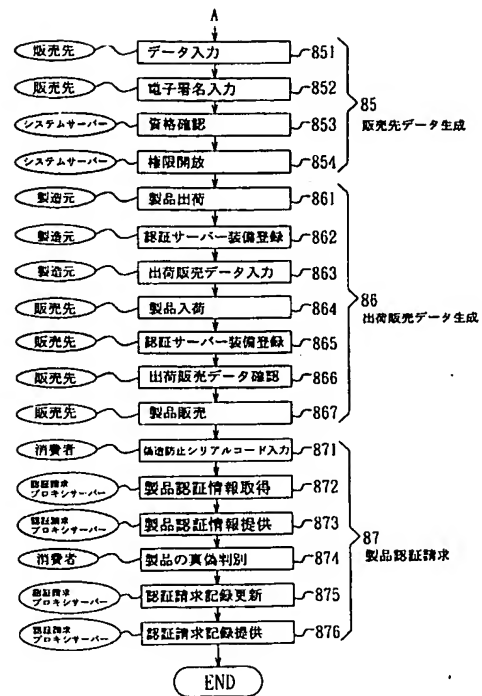
【図 2】



【図 3】



【図 4】



【図 5】

124  
MSW95TW0115200

【図 6】

